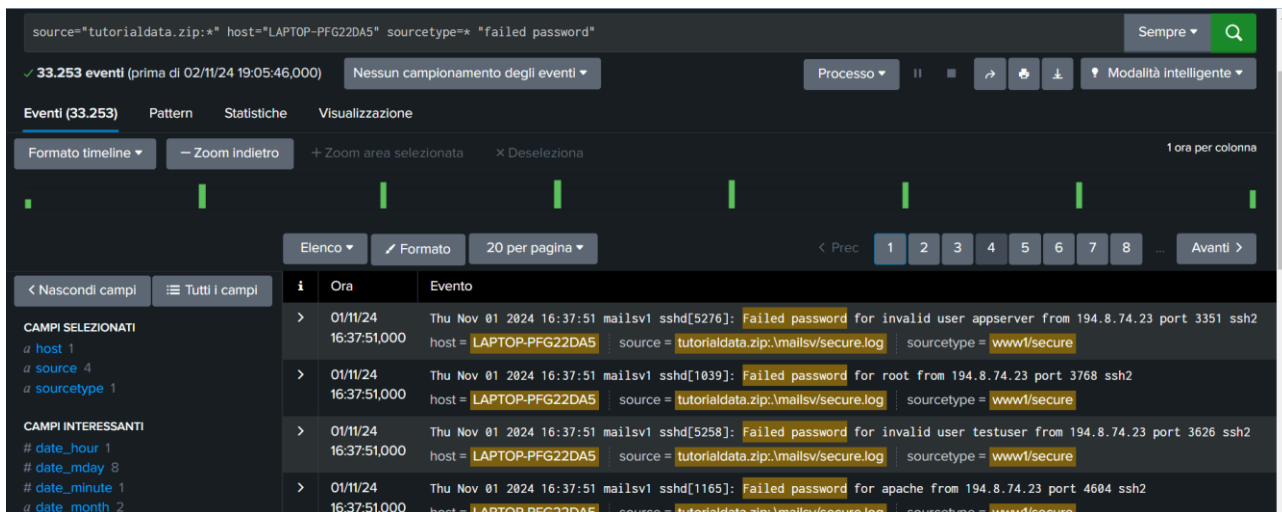


W24D4



Conclusione:

Dall'immagine del log, possiamo dedurre quanto segue:

- **Eventi:** Sono stati registrati numerosi tentativi falliti di accesso al sistema.
- **Host:** Tutti gli eventi provengono dallo stesso computer, "LAPTOP-PFG22DA5".
- **Tipo di Accesso:** I tentativi riguardano principalmente l'accesso tramite SSH (Secure Shell), un protocollo comunemente utilizzato per la connessione remota a sistemi Unix-like.
- **Utenti e Servizi:** Gli attacchi sembrano rivolti a utenti e servizi specifici (appserver, root, testuser, apache), suggerendo che l'attaccante potrebbe avere informazioni specifiche sulla configurazione del sistema.
- **Indirizzo IP:** Tutti i tentativi provengono dallo stesso indirizzo IP (194.8.74.23), il che potrebbe indicare un singolo attaccante o un attacco proveniente da una rete compromessa.

Conclusioni

Sulla base di queste informazioni, possiamo trarre le seguenti conclusioni:

1. **Attacco in Corso:** Il numero elevato di tentativi falliti in un breve periodo di tempo indica chiaramente un attacco in corso.
2. **Brute Force:** La natura degli attacchi (tentativi di accesso con password errate per diversi utenti) suggerisce che l'attaccante stia utilizzando una tecnica di brute force, ovvero provando sistematicamente diverse combinazioni di password.
3. **Informazioni Preliminari:** L'attaccante sembra avere alcune informazioni preliminari sul sistema, come l'esistenza di specifici utenti e servizi, il che potrebbe indicare una fase di ricognizione preliminare all'attacco.
4. **Minaccia alla Sicurezza:** Questo tipo di attacco rappresenta una seria minaccia per la sicurezza del sistema, in quanto l'attaccante potrebbe riuscire a ottenere l'accesso non autorizzato al sistema e a sfruttarlo per scopi malevoli.

Possibili Misure da Adottare

Per mitigare questa minaccia, si suggeriscono le seguenti azioni:

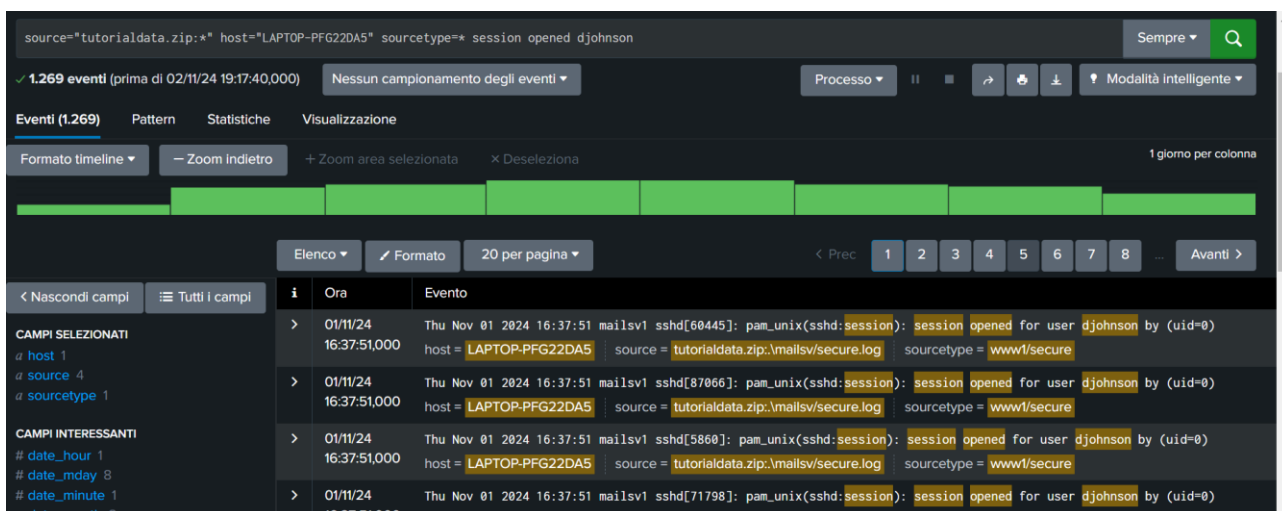
- **Bloccare l'Indirizzo IP:** Bloccare temporaneamente o definitivamente l'indirizzo IP sorgente dei tentativi di intrusione.
- **Rendere più Sicure le Password:** Impostare password forti e uniche per tutti gli utenti e abilitare l'autenticazione a due fattori.
- **Limitare i Tentativi di Accesso:** Configurare il sistema per bloccare automaticamente gli account dopo un numero specificato di tentativi di accesso falliti.
- **Aggiornare il Software:** Assicurarsi che tutti i software del sistema siano aggiornati con le ultime patch di sicurezza.
- **Monitorare Costantemente i Log:** Continuare a monitorare i log alla ricerca di ulteriori attività sospette.
- **Analizzare i Log Dettagliatamente:** Utilizzare strumenti di analisi dei log per identificare eventuali pattern o anomalie che potrebbero indicare altri tipi di attacchi.

Considerazioni Aggiuntive

- **Tipo di Sistema Compromesso:** Sarebbe utile determinare il tipo di sistema che è stato attaccato (server, workstation, dispositivo IoT) per adottare misure di sicurezza più mirate.
- **Motivazione dell'Attacco:** Capire la motivazione dell'attaccante (spionaggio industriale, vandalismo, estorsione) può aiutare a prevenire futuri attacchi.
- **Rete Compromessa:** Se l'indirizzo IP sorgente appartiene a una rete compromessa, potrebbe essere necessario contattare il provider di servizi Internet (ISP) per segnalare il problema.

Conclusioni Finali

L'analisi dei log ha evidenziato un chiaro tentativo di intrusione nel sistema. È fondamentale agire rapidamente per mitigare la minaccia e prevenire ulteriori attacchi. Un approccio multistrato alla sicurezza, combinato con un monitoraggio costante dei log, è essenziale per proteggere i sistemi informatici da minacce sempre più sofisticate.



The screenshot shows a log analysis interface with a search bar at the top containing the query: `source="tutorialdata.zip:*" host="LAPTOP-PFG22DA5" sourcetype=* session opened djohnson`. Below the search bar, there are filters and a timeline view. The main table displays search results for 'session opened djohnson'.

	Ora	Evento
>	01/11/24 16:37:51,000	Thu Nov 01 2024 16:37:51 mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = LAPTOP-PFG22DA5 source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	01/11/24 16:37:51,000	Thu Nov 01 2024 16:37:51 mailsv1 sshd[87066]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = LAPTOP-PFG22DA5 source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	01/11/24 16:37:51,000	Thu Nov 01 2024 16:37:51 mailsv1 sshd[5860]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = LAPTOP-PFG22DA5 source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure
>	01/11/24 16:37:51,000	Thu Nov 01 2024 16:37:51 mailsv1 sshd[71798]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) host = LAPTOP-PFG22DA5 source = tutorialdata.zip:mailsv/secure.log sourcetype = www/secure

Conclusione:

Dall'immagine, possiamo dedurre i seguenti punti chiave:

- **Fonte dei Dati:** Il log proviene da un file compresso denominato "tutorialdata.zip" e sembra essere relativo a un'attività di login.
- **Host:** L'attività è stata registrata sul computer "LAPTOP-PFG22DA5".
- **Utente:** L'utente che ha effettuato il login è "djohnson".
- **Evento:** L'evento registrato è l'apertura di una sessione.
- **Timestamp:** Gli eventi sono datati al 01/11/24 alle 16:37:51.
- **Sourcetype:** Il tipo di sorgente è associato a file di log di sicurezza.

Possibili Conclusioni

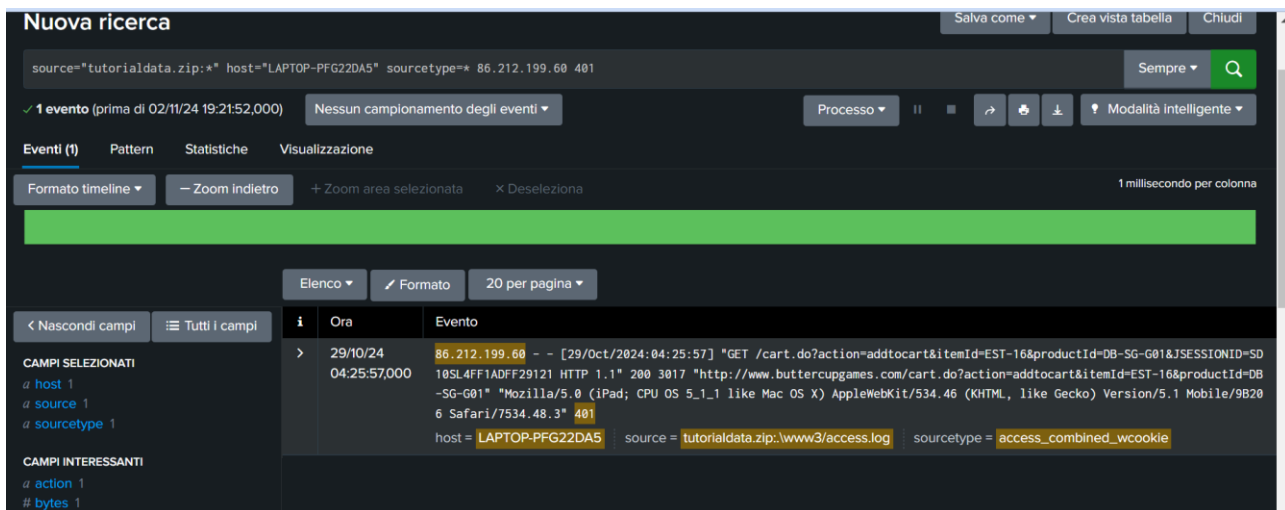
Sulla base di queste informazioni, possiamo formulare alcune ipotesi:

1. **Tentativi di Login Multipli:** Il fatto che ci siano più eventi di login nello stesso timestamp potrebbe indicare:
 - **Script o Tool Automatici:** Qualcuno potrebbe aver utilizzato uno script o uno strumento per effettuare più tentativi di login in rapida successione.
 - **Errore di Registrazione:** Potrebbe esserci un problema nel sistema di logging che ha causato la duplicazione degli eventi.
2. **Attività Normale:** Se l'utente "djohnson" ha effettivamente effettuato più login in quel momento specifico, potrebbe essere un'attività del tutto normale, ad esempio per accedere a diverse risorse o applicazioni.
3. **Possibile Compromissione:** Sebbene non sia possibile affermarlo con certezza sulla base di questi dati, un'attività di login anomala, soprattutto se accompagnata da altri eventi sospetti (come accessi a file sensibili o modifiche alle configurazioni), potrebbe indicare un tentativo di intrusione.

Analisi Più Approfondita

Per trarre conclusioni più definitive, sarebbe necessario:

- **Esaminare l'intero File di Log:** Cercare eventuali pattern anomali, come un numero eccessivo di tentativi di login falliti, accessi da indirizzi IP sconosciuti o attività insolite durante la sessione.
- **Correlare i Dati con Altre Fonti:** Confrontare i dati del log con altre fonti, come i registri di sistema, i firewall e i sistemi di rilevamento delle intrusioni, per individuare eventuali anomalie.
- **Analizzare il Contesto:** Considerare il contesto in cui si è verificata l'attività. Ad esempio, se il sistema è stato recentemente compromesso, è più probabile che i login multipli siano dovuti a un attacco.



Conclusione:

1. Tipo di Evento

Il log rappresenta un tentativo di accesso non autorizzato che ha ricevuto una risposta di tipo **401 (Unauthorized)**. Questo codice di stato HTTP indica che l'accesso richiesto richiede autenticazione e che la richiesta è fallita perché l'autenticazione non è stata fornita correttamente o non è stata riconosciuta.

2. Indirizzo IP

L'indirizzo IP sorgente del tentativo di accesso è **86.212.199.60**, che è stato registrato mentre cercava di accedere a una risorsa del server.

3. Risorsa Richiesta

La risorsa a cui si tentava di accedere è `/cart.do?action=addtocart&itemId=...`, suggerendo che l'IP stava cercando di interagire con il carrello di un'applicazione web. Questa attività potrebbe rappresentare un tentativo di esplorazione o manipolazione non autorizzata della funzionalità del carrello.

4. Dettagli del Client

L'User-Agent indica che la richiesta è stata effettuata utilizzando un browser su un dispositivo iPad (AppleWebKit/534.46). Questo può essere utile per identificare eventuali modelli di attacco da dispositivi mobili o browser specifici.

5. Host

L'host coinvolto è identificato come **LAPTOP-PFG22DA5**, il che suggerisce che la richiesta è stata monitorata o è stata tentata su un host locale o monitorato dalla macchina stessa.

Conclusioni e Azioni Consigliate

- **Monitoraggio Aggiuntivo:** Poiché questo IP ha tentato di accedere senza autorizzazione, è consigliabile monitorare ulteriori attività provenienti da esso per verificare se vi siano altri tentativi simili.
- **Verifica della Sicurezza:** La funzionalità del carrello potrebbe essere un obiettivo di attacchi; controllare e rafforzare la protezione di queste funzioni può essere utile.
- **Logging e Alert:** Implementare regole di alert in Splunk per notificare in tempo reale tentativi di accesso non autorizzato, soprattutto se ripetuti.

Nuova ricerca Salva come Crea vista tabella Chiudi

source="tutorialdata.zip:*" sourcetype="*" "Failed password" ip="*" | stats count by ip | where count > 5 Da 01/11/24 fino a 30/11/24 Q

✓ 4.564 eventi (01/11/24 00:00:00,000 - 01/12/24 00:00:00,000) Nessun campionamento degli eventi Processo II ■ ↻ 📄 ⬇ 🔍 Modalità intelligente

Eventi Pattern **Statistiche (137)** Visualizzazione

20 per pagina Formato Anteprima < Prec 1 2 3 4 5 6 7 Avanti >

ip	count
107.3.146.207	66
108.65.113.83	18
109.169.32.135	86
110.159.208.78	6
112.111.162.4	10
117.21.246.164	64
12.130.60.4	40
12.130.60.5	32
121.254.179.199	6
121.9.245.177	58
123.196.113.11	20
123.30.108.208	64
124.160.192.241	58
125.17.14.100	28
128.241.220.82	74
130.253.37.97	26

Conclusione:

1. Elevata Attività di Accesso Fallito

La query identifica gli indirizzi IP che hanno avuto più di 5 tentativi di accesso falliti ("Failed password"). Questo suggerisce che alcuni IP potrebbero essere coinvolti in attività sospette come attacchi di forza bruta o tentativi di accesso non autorizzato.

2. Indirizzi IP Frequenti

Alcuni IP hanno un numero significativamente alto di tentativi falliti, come 107.3.146.207 (66 tentativi) e 169.169.32.135 (86 tentativi). Questi indirizzi IP potrebbero essere prioritari per ulteriori indagini e verifiche di sicurezza.

3. Distribuzione delle Attività

La presenza di vari IP con numeri di tentativi di accesso falliti distribuiti su più righe indica che questi eventi non sono limitati a un singolo attaccante o a un solo indirizzo IP. Questo potrebbe

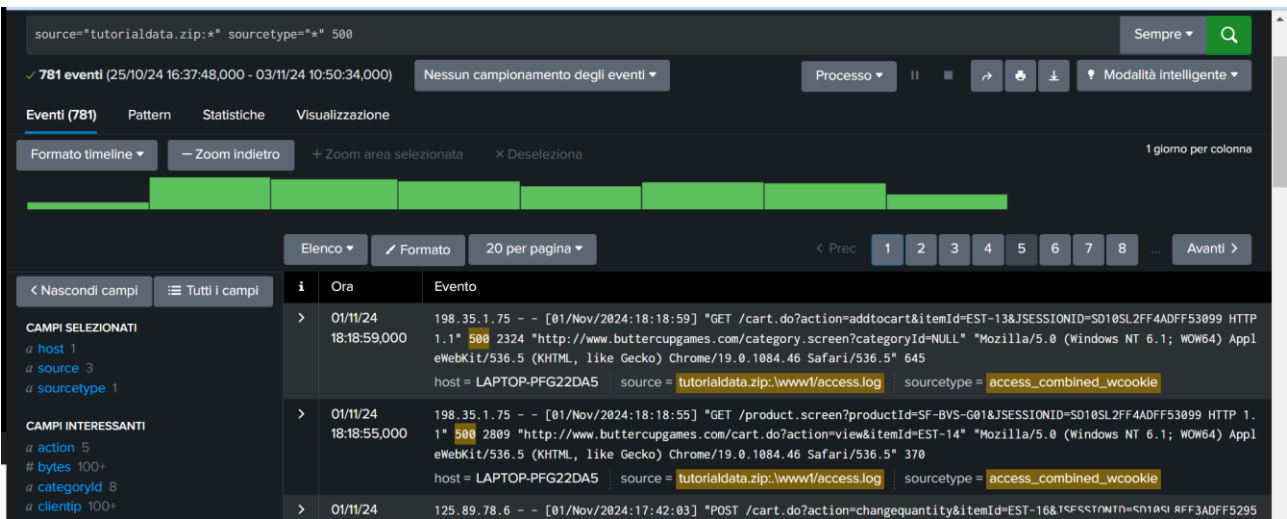
suggerire un comportamento più ampio, come un attacco distribuito o tentativi non coordinati da più fonti.

4. Rischio Potenziale

Indirizzi IP con un alto numero di tentativi potrebbero essere indicativi di un rischio per la sicurezza. Monitorare e analizzare ulteriormente questi IP è cruciale per evitare compromissioni future.

Azioni Consigliate

1. **Bloccare o Monitorare gli IP:** Implementare regole di firewall o altre misure per limitare l'accesso da IP con alto numero di tentativi falliti.
2. **Analisi Geografica:** Eseguire una mappatura geografica degli IP per identificare se i tentativi provengono da aree non attese.
3. **Revisionare le Policy di Sicurezza:** Verificare se i sistemi di autenticazione possono essere migliorati per prevenire questi tentativi, come l'adozione di misure anti-brute-force.
4. **Alert e Logging Avanzati:** Creare alert automatici in Splunk per notificare quando un IP supera una soglia critica di tentativi di accesso falliti.



Conclusione:

1. Tipo di Evento

L'errore "500" indica un "Internal Server Error", il che significa che si è verificato un problema lato server. Questo può essere causato da varie ragioni, come malfunzionamenti nei servizi back-end, errori nella logica del server, o problemi di configurazione.

2. Indirizzi IP

Gli indirizzi IP mostrati, come 198.35.1.75 e 125.89.78.49, indicano le fonti da cui provengono le richieste che hanno generato gli errori. Questi IP possono essere ulteriormente analizzati per capire se sono fonti affidabili o se provengono da aree geografiche o provider inusuali.

3. Percorsi e Richieste

I log includono richieste HTTP come `GET /cart.do?action=addtocart&itemId=EST-13`. Questi dettagli sono utili per capire quali endpoint o funzionalità dell'applicazione stanno causando errori. L'endpoint `/cart.do` potrebbe indicare un problema legato alla gestione del carrello, come errori nell'aggiunta di prodotti o nella gestione delle sessioni.

4. Orario degli Eventi

Gli eventi sono distribuiti su più giorni e si può osservare una certa frequenza di errori. Un'analisi più dettagliata delle fasce orarie può indicare se questi errori avvengono durante periodi specifici di carico maggiore, come orari di punta o manutenzioni.

5. User-Agent

Le informazioni sui browser utilizzati (`Mozilla/5.0`, `Safari/536.5`) indicano che le richieste provengono da client comuni e non sembrano sospette di per sé. Tuttavia, se si identificano user-agent insoliti o automazioni, questo potrebbe segnalare attività anomale o tentativi di abuso.

Possibili Azioni di Approfondimento

- **Analisi della Causa Radice:** Verificare i log applicativi per capire il motivo per cui gli errori interni si verificano su endpoint specifici.
- **Verifica delle Origini IP:** Controllare se gli indirizzi IP sono associati a utenti legittimi o a tentativi di accesso anomali.
- **Monitoraggio delle Tendenze:** Creare dashboard per monitorare la frequenza degli errori 500 e identificare picchi o variazioni significative nel tempo.

Raccomandazioni

- **Controllare la Logica Server-Side:** Analizzare e correggere le parti di codice che gestiscono le richieste che generano errori interni.
- **Implementare Log Dettagliati:** Aggiungere logging per comprendere meglio i flussi interni del server quando si verificano questi errori.
- **Configurazione del Server:** Verificare che il server e i suoi componenti siano configurati correttamente e aggiornati per prevenire errori imprevisti.